



DEFENSE INFORMATION SYSTEMS AGENCY

JOINT INTEROPERABILITY TEST COMMAND

P.O. BOX 12798

FORT HUACHUCA, ARIZONA 85670-2798

IN REPLY
REFER TO:

Battlespace Communications Portfolio (JTE)

05 Apr 07

MEMORANDUM FOR DISTRIBUTION

SUBJECT: Special Interoperability Test Certification of Techguard PoliWall for Internet Protocol Version 6 (IPv6) Capability

References: (a) DoDD 4630.5, "Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)," 5 May 2004
(b) CJCSI 6212.01D, "Interoperability and Supportability of Information Technology and National Security Systems," 8 March 2006

1. References (a) and (b) establish the Joint Interoperability Test Command (JITC), as the responsible organization for interoperability test certification. Additional references are provided in enclosure 1.
2. Techguard PoliWall, hereinafter referred to as the device under test (DUT), met the Internet Protocol (IP) Version 6 (IPv6) Capable requirements and is certified for listing on the Department of Defense (DoD) IPv6 Approved Products List as IPv6 Capable as a Network Appliance. Reference (c) provides the IPv6 network appliance profile. The DUT successfully completed the related IPv6 Performance and Interoperability portions of the DoD IPv6 Generic Test Plan Version 2, September 2006. This certification expires upon changes that could affect interoperability, but no later than three years from the date of this memorandum.
3. This special certification is based on IPv6 Capable testing conducted by JITC at Fort Huachuca, Arizona. Testing was conducted at JITC's Advanced IP Technology Laboratory from 19 to 23 February 2007. Conformance testing was completed by Techguard and was verified in the Letter of Conformance from Techguard dated 29 January 2007. Enclosure 2 documents the test results and describes the DUT. Users should verify interoperability before deploying the DUT in an environment that varies significantly from that described.
4. The DUT's interoperability test summary is found in table 1. The interoperability test status is based on the DUT's ability to meet DoD IPv6 Standard Profiles for IPv6 Capable Products, specifically the network appliance profile. The DUT's equipment list is in table 2.

JITC Memo, JTE, Special Interoperability Test Certification of Techguard PoliWall for Internet Protocol Version 6 (IPv6) Capability

Table 1. DUT Interoperability Test Summary

Techguard PoliWall			
Functional Category	Critical	Verified	Remarks
Core IPv6 Functionality	Yes	Yes	
Connection Technologies	Yes	Yes	
Transition Mechanisms	Yes	Yes	
Common Network Applications	No	No	
Information Assurance	Yes	Yes	
Mobility	No	No	
Quality of Service	No	No	
Multicasting	No	No	
Network Operations and Management	No	No	
LEGEND: DUT Device Under Test IPv6 Internet Protocol Version 6			

Table 2. DUT Equipment Listing

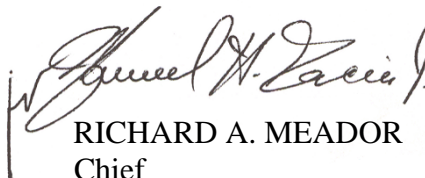
Techguard PoliWall		
Equipment Name	OS	Version
Techguard PoliWall	PoliWall	1.20.04
LEGEND: DUT Device Under Test OS Operating System		

5. No detailed test report was written in accordance with the DoD IPv6 Master Test Plan. JITC distributes interoperability information via the JITC Electronic Report Distribution (ERD) system, which uses Unclassified-But-Sensitive Internet Protocol Router Network (NIPRNet) e-mail. More comprehensive interoperability status information is available via the JITC System Tracking Program (STP). The STP is accessible by .mil/gov users on the NIPRNet at <https://stp.fhu.disa.mil>. Test reports, lessons learned, and related testing documents and references are on the JITC Joint Interoperability Tool (JIT) at <http://jit.fhu.disa.mil> (NIPRNet), or <http://199.208.204.125> (SIPRNet). Information related to IPv6 Capable testing is on the DoD IPv6 Approved Products List at http://jitc.fhu.disa.mil/adv_ip/register/register.html.

6. The JITC point of contact is Captain Richard J. Duncan, DSN 821-0154, commercial (520) 533-0154, or e-mail richard.j.duncan@disa.mil.

FOR THE COMMANDER:

2 Enclosures a/s



RICHARD A. MEADOR
Chief
Battlespace Communications Portfolio

JITC Memo, JTE, Special Interoperability Test Certification of Techguard PoliWall for Internet Protocol Version 6 (IPv6) Capability

Distribution:

Joint Staff J6I, Room 1E596, Pentagon, Washington, DC 20318-6000
Office of Assistant Secretary of Defense (NII)/DoD CIO, Crystal Mall 3, 7th Floor, Suite 7000,
1851 S. Bell St., Arlington, VA 22202
Defense Information Systems Agency, Net-Centricity Requirements and Assessment Branch,
ATTN: GE333, Room 244, P.O. Box 4502, Falls Church, VA 22204-4502
Defense Information Systems Agency, Standards and Engineering Branch, ATTN: GE331,
Bldg 283, Fort Monmouth, NJ 07703
Air Force Communications Agency/ECSS, ATTN: IPv6 Transition Office, 203 Losey St., Scott
Air Force Base, IL 62225
Navy IPv6 Transition Project Office, ATTN: SPAWAR 053 OT1, 4301 Pacific Highway,
San Diego, CA 92110-3127
U.S. Army, ATTN: CIO-G-6, SAIS-AOT, 107 Army Pentagon, Washington, DC 20310-0107
U.S. Marine Corps (C4ISR), MARCORSYSCOM, 2200 Lester St., Quantico, VA 22134-5010
DOT&E, Net-Centric Systems and Naval Warfare, 1700 Defense Pentagon,
Washington, DC 20301-1700
Joint Interoperability Test Command, Liaison, ATTN: TED/JT1, 2W24-8C, P.O. Box 4502,
Falls Church, VA 22204-4502
Office of Chief of Naval Operations (N71CC2), CNO N6/N7, 2000 Navy Pentagon,
Washington, DC 20350
Headquarters U.S. Air Force, AF/XICF, 1800 Pentagon, Washington, DC 20330-1800
Department of the Army, Office of the Secretary of the Army, CIO/G6,
ATTN: SAIS-IOQ, 107 Army Pentagon, Washington, DC 20310-0107
U.S. Coast Guard, CG-64, 2100 2nd St. SW, Washington, DC 20593
Defense Intelligence Agency, 2000 MacDill Blvd., Bldg 6000, Bolling AFB,
Washington, DC 20340-3342
National Security Agency, ATTN: DT, Suite 6496, 9800 Savage Road,
Fort Meade, MD 20755-6496
Director, Defense Information Systems Agency, ATTN: GS235, Room 5W24-8A,
P.O. Box 4502, Falls Church, VA 22204-4502
Office of Under Secretary of Defense, AT&L, Room 3E144, 3070 Defense Pentagon,
Washington, DC 20301
U.S. Joint Forces Command, J68, Net-Centric Integration, Communications, and
Capabilities Division, 1562 Mitscher Ave., Norfolk, VA 23551-2488

ADDITIONAL REFERENCES

- (c) DISR, "DoD IPv6 Standard Profiles for IPv6 Capable Products v1," 1 June 2006
- (d) "DISR Global Information Grid (GIG) Convergence Master Plan (GCMP), Version 5.25," 29 March 2006
- (e) Department of Defense (DoD) Internet Protocol Version 6 (IPv6) Transition Office (DITO), "DoD Chief Information Officer (CIO) Memo, IPv6," 9 June 2003
- (f) DITO, "DoD CIO Memo, IPv6 Interim Transition Guidance," 29 September 2003
- (g) DITO, "DoD IPv6 Master Test Plan, Version 2," September 2006
- (h) Joint Interoperability Test Command, "DoD IPv6 Generic Test Plan Version 2," September 2006

INTERNET PROTOCOL VERSION 6 CAPABLE TESTING SUMMARY

1. SYSTEM TITLE. Techguard PoliWall.

2. PROPONENT. Department of Defense (DoD) Internet Protocol (IP) Version 6 (IPv6) Transition Office (DITO).

3. PROGRAM MANAGER/USER POC. DITO, Defense Information Systems Agency, Attn: GE36 Thomas McCrickard, P.O. Box 4502, Arlington, VA 22204-4502, (703) 882-0241, e-mail: tom.mccrickard@disa.mil.

4. TESTER. Captain Richard J. Duncan, Joint Interoperability Test Command (JITC), P.O. Box 12798, Fort Huachuca, AZ 85670-2798, DSN: 821-0154, commercial: (520) 533-0154, e-mail: richard.j.duncan@disa.mil.

5. DEVICE UNDER TEST DESCRIPTION. The Techguard PoliWall, hereinafter referred to as the device under test (DUT), was configured to support single and dual stack operation of the IP Version 4 (IPv4)/IPv6 protocols.

6. OPERATIONAL ARCHITECTURE. The operational architecture was the simulated Network Boundary as depicted in figure 2-1.

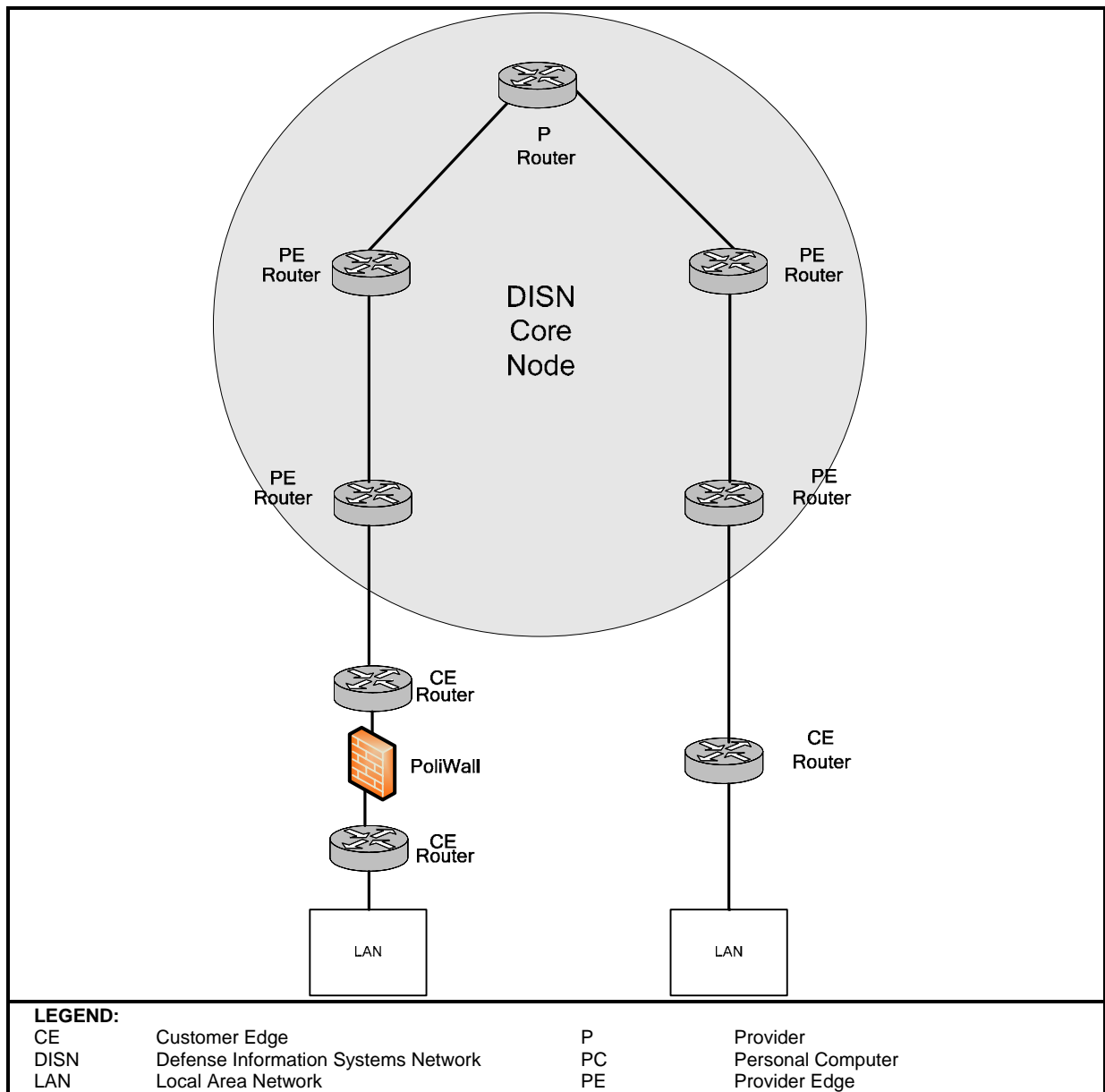


Figure 2-1. PoliWall Test Network

7. REQUIRED DEVICE INTERFACES. All IPv6 testing must follow the requirements of the DoD Information Technology Standards Registry (DISR) DoD IPv6 Standard Profiles for IPv6 Capable Products v1, 1 June 2006, and are tested in accordance with the DoD IPv6 Generic Test Plan Version 2, September 2006. The IPv6 network appliance profile requirements specific to the DUT are conformance, performance, and interoperability and are listed in table 2-1.

Table 2-1. IPv6 Capability Requirements and Status

Techguard PoliWall								
RFC	RFC Title	Testing Completed			Network Appliance		Implemented	Comments
		Conformance	Performance	Interoperability	Requirement	Met/Not Met		
Core IPv6 Functionality								
1981	Path Maximum Transmission Unit Discovery for IPv6	Stated in LoC	No Performance Test Required	Yes	R	Met	Yes	
2460	Internet Protocol version 6 (IPv6) Specification	Stated in LoC	No Performance Test Required	Yes	R	Met	Yes	
2461	Neighbor Discovery for IP version 6 (IPv6)	Stated in LoC	No Performance Test Required	Yes	R	Met	Yes	
2462	IPv6 Stateless Address Auto configuration	Stated in LoC	No Performance Test Required	Yes	R	Met	Yes	
4291	IPv6 Addressing Architecture	Stated in LoC	No Performance Test Required	Yes	R	Met	Yes	
4007	IPv6 Scoped Address Architecture	Stated in LoC	No Performance Test Required	Yes	R	Met	Yes	
4301	Security Architecture for Internet Protocol	Stated in LoC	No Performance Test Required	Yes	R	Met	Yes	
4193	Unique Local IPv6 Unicast Addresses	Stated in LoC	No Performance Test Required	Yes	R	Met	Yes	
4443	Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification	Stated in LoC	No Performance Test Required	Yes	R	Met	Yes	
Connection Technologies								
2464	Transmission of IPv6 Packets over Ethernet Networks	Stated in LoC	No Performance Test Required	Yes	R	Met	Yes	
Transition Mechanisms								
4213	Transition Mechanisms for IPv6 Host and Routers	Stated in LoC	Yes	Yes	R	Met	Yes	

Table 2-1. IPv6 Capability Requirements and Status (continued)

Techguard PoliWall								
RFC	RFC Title	Testing Completed			Network Appliance		Implemented	Comments
		Conformance	Performance	Interoperability	Requirement	Met/Not Met		
Information Assurance								
2407	The Internet Security Domain of Interpretation for ISAKMP	Stated in LoC	No Performance Test Required	Yes	R	Met	Yes	
2408	Internet Security Association and Key Management Protocol	Stated in LoC	No Performance Test Required	Yes	R	Met	Yes	
2409	Internet Key Exchange (IKE)	Stated in LoC	No Performance Test Required	Yes	R	Met	Yes	
4109	Algorithms for Internet Key Exchange Version 1 (IKEv1)	Stated in LoC	No Performance Test Required	Yes	R	Met	Yes	
4302	IP Authentication Header	Stated in LoC	No Performance Test Required	Yes	R	Met	Yes	
4303	IP Encapsulating Security Payload (ESP)	Stated in LoC	No Performance Test Required	Yes	R	Met	Yes	
4305	Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)	Stated in LoC	No Performance Test Required	Yes	R	Met	Yes	
4308	Cryptographic Suites for IPsec	Stated in LoC	No Performance Test Required	Yes	R	Met	Yes	
LEGEND: IP Internet Protocol IPSec Internet Protocol Security IPv6 IP Version 6 ISAKMP Internet Security Association and Key Management Protocol LoC Letter of Conformance R Required RFC Request for Comments								

8. TEST NETWORK DESCRIPTION. The DUT was tested as part of a simulated Network Boundary managed by the Advanced IP Technology Laboratory at JITC, and configured as shown in figure 2-2.

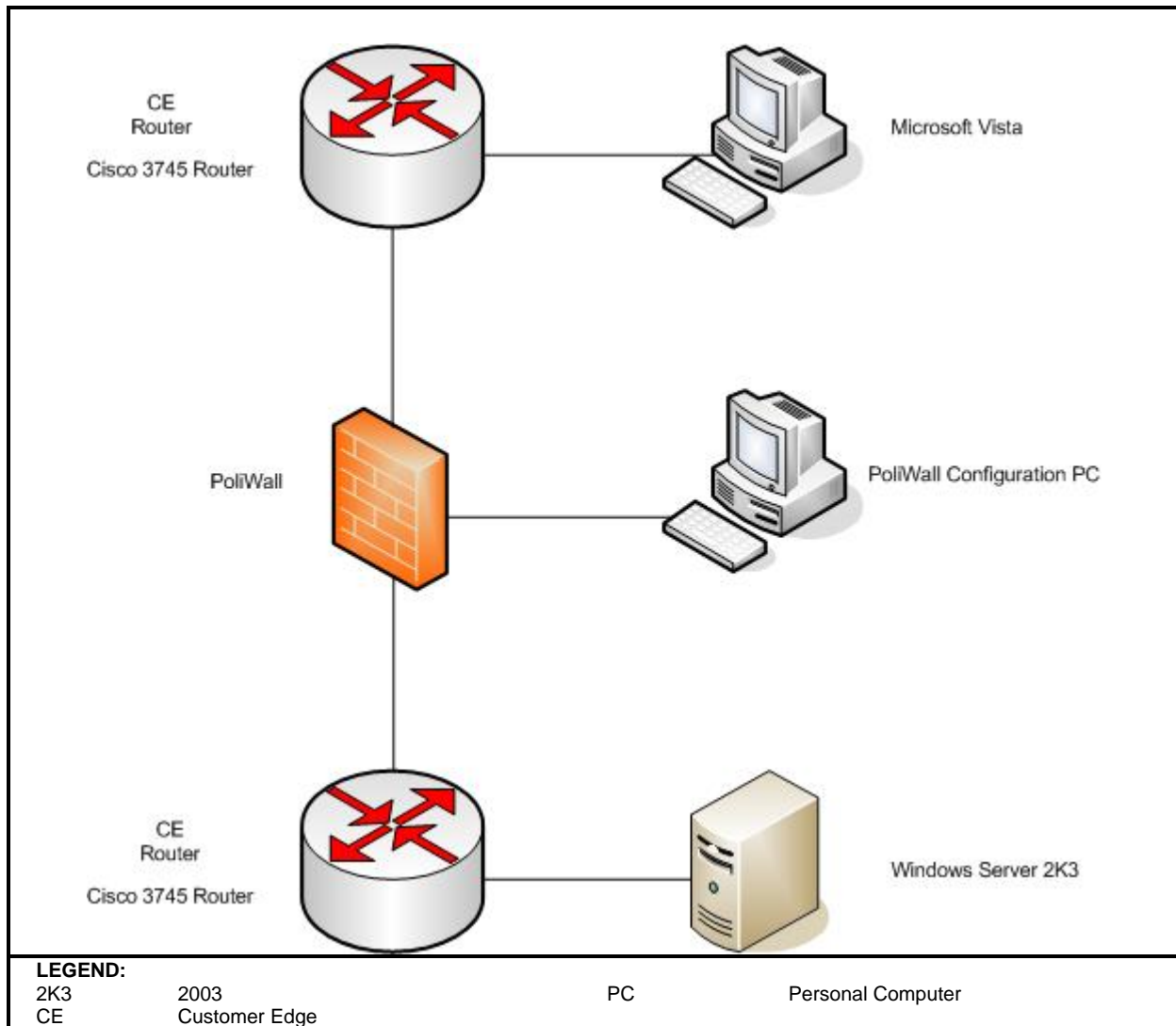


Figure 2-2. PoliWall Test Network

9. DEVICE CONFIGURATIONS. Table 2-2 provides hardware and software components used in the test network.

Table 2-2. Test Configuration Hardware and Software

Equipment Name	Model Number	IOS/OS Version(s)
Hardware		
Cisco 3745 Router	CISCO3745	12.3(14)T2
Cisco 3745 Router	CISCO3745	12.4(4)T1
Dell Power Edge Server	2850	Microsoft Windows Server 2003
Dell Power Edge Server	2650	Microsoft Windows Vista Enterprise
Dell Power Edge Server	4600	RedHat Enterprise 4
Gateway Laptop	450ROG	Microsoft Windows XP
Techguard PoliWall	PoliWall	1.20.40
Software		
Microsoft Windows Vista	N/A	Enterprise
Microsoft Windows Server	N/A	2003
Redhat Enterprise	N/A	4
Microsoft Windows XP	N/A	Professional
Wireshark	N/A	V.0.99.2
LEGEND: IOS Internetwork Operating System OS Operating System N/A Not Applicable V Version		

10. TEST LIMITATIONS. None.

11. TEST RESULTS.

a. Core IPv6 Functionality.

Reference test cases E.1.1, E.1.2, and E.4.3. The Request for Comments (RFC) 1981 Path Maximum Transmission Unit Discovery for IPv6 is necessary for proper IPv6 implementations. It acts as a mechanism to determine the maximum size of packets to traverse the network without fragmentation. The DUT met the test requirement.

Reference test cases E.4.3, E.5.2, E.5.8, E.5.9, E.5.10, E.5.16, and E.5.17. The RFC 2460 is the base specification of the IPv6 protocol. It specifies a number of parameters that enable successful completion of IPv6 traffic addressing and control. The DUT met the test requirement.

Reference test cases E.1.1, E.1.3, E.1.5, E.4.3, E.5.5, and E.5.7. The RFC 2461 specifies the neighbor discovery function that is similar to address resolution protocol in IPv4. It is necessary for implementing neighbor solicitations and neighbor advertisements within IPv6. The DUT met the test requirement.

Reference test cases E.1.1, E.1.4, E.4.3, E.5.5, and E.6.4. The RFC 2462 specifies how a host auto-configures its interfaces in IPv6. These steps include determining whether the source addressing should be stateless or stateful, whether the information obtained should be solely the address or include other information, and Duplicate

Address Detection. The DUT met the test requirement.

Reference test case E.1.6. The RFC 4291 defines the specifications for the addressing architecture of the IPv6 protocol. The definitions cover unicast addresses, anycast addresses, and multicast addresses. The DUT met the test requirement.

Reference test case E.1.7. The RFC 4007 defines the nature and characteristics for the usage of IPv6 addresses of different scopes. The DUT met the test requirement.

Reference test case E.1.8. The RFC 4301 defines the security architecture for IP. The document defines what IP Security is and how it works. The DUT met the test requirement.

Reference test case E.1.9. The RFC 4193 defines the address format and how it is globally unique. Local IPv6 unicast addressing is intended to be used for local communications and is not expected to be routed to the Internet. The DUT met the test requirement.

Reference test cases E.1.1, E.5.3, E.5.6, and E.5.16. The RFC 4443 identifies Internet Control Message Protocol messages for the IPv6 protocol. It includes message format and identifies two types of messages: error and informational. The DUT met the test requirement.

b. Connection Technologies.

Reference test cases D.2.1, E.2.1, and E.4.3. The RFC 2464 specifies the frame format for transmission of an IPv6 link-local addresses and a stateless auto-configured addresses on Ethernet networks. The DUT met the test requirement.

c. Transition Mechanisms.

Reference test cases D.3.1, D.3.2, D.3.3, E.3.1, E.3.2, and E.3.3. The RFC 4213 specifies IPv4 co-existence mechanisms that can be implemented by IPv6 devices. The DUT met the test requirement.

d. Information Assurance.

Reference test case E.5.18. The RFC 2407 Internet Security Association and Key Management Protocol (ISAKMP) defines a framework for security association management and cryptographic key establishment for the Internet. This framework consists of defined exchanges, payloads, and processing guidelines that occur within a given Domain of Interpretation. The DUT met the test requirement.

Reference test case E.5.20. The RFC 2408 describes a protocol utilizing security concepts necessary for establishing Security Associations and cryptographic keys in an Internet environment. The DUT met the test requirement.

Reference test case E.5.10. For the RFC 2409 Internet Key Exchange, the ISAKMP provides a framework for authentication and key exchange, but does not define the two. The ISAKMP is designed to be key exchange independent. The DUT met the test requirement.

Reference test case E.5.21. The RFC 4109 Algorithms for Internet Key Exchange version (IKEv1) defines an Internet standards track protocol for the Internet community. The DUT met the test requirement.

Reference test case E.5.22. The RFC 4302 IP Authentication Header (AH) is used to provide connectionless integrity and data origin authentication for IP datagrams, and provides protection against replays. The DUT met the test requirement.

Reference test case E.5.23. In the RFC 4303 IP Encapsulating Security Payload (ESP), the ESP header is designed to provide a mix of security services in IPv4 and IPv6. The DUT met the test requirement.

Reference test case E.5.24. The RFC 4305 defines the requirements for ESP and AH. The DUT met the test requirement.

Reference test case E.5.9. The RFC 4308 defines the two different types of user interface suites. The first suite is called “Virtual Private Network (VPN)-A” and includes ESP, 3-Data Encryption Standard and Secure Hash Algorithm-1. The second suite is called “VPN-B” and includes ESP, Advanced Encryption Standard with 128-bit keys. The RFC states these suites are optional non-mandatory suites. The DUT met the test requirement.

e. Conclusions. The Techguard PoliWall met all the test requirements of a network appliance.

12. TEST AND ANALYSIS REPORT. No detailed test report was written in accordance with the DoD IPv6 Master Test Plan. All test data is maintained in the Advanced IP Technology Laboratory and is available upon request. This assessment is available on the Joint Interoperability Tool (JIT). The JIT homepage is <http://jit.fhu.disa.mil> (NIPRNet), or <http://199.208.204.125/> (SIPRNet). The JIT has links to JITC interoperability documents to provide the DoD community, including the warfighter in the field, easy access to the latest interoperability information. System interoperability status information is available via the JITC System Tracking Program (STP). The STP is accessible by .mil/.gov users on the NIPRNet at: <https://stp.fhu.disa.mil/>.